

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

Electronic items located inside a carrying case,
recovered in Building #197, Washington Navy Yard,
Southwest, Washington, D.C.

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
SEE ATTACHMENT A

located in the _____ District of _____ Columbia _____, there is now concealed *(identify the person or describe the property to be seized)*:
SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Section 1111	Murder
18 U.S.C. Section 1113	Attempted Murder
18 U.S.C. Section 1114	Killing or Attempting to Kill an Officer/Employee of United States

The application is based on these facts:

SEE ATTACHED AFFIDAVIT.

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Sarah Jones

Printed name and title

Sworn to before me and signed in my presence.

Date: 09/17/2013

Judge's signature

City and state: District of Columbia

Magistrate Judge John M. Facciola

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF)	
)	
A LENOVO THINKPAD T500 LAPTOP)	
COMPUTER HAVING SERIAL NUMBER)	Case No.:
L3-B0317 09/02 AND)	
PRODUCT ID NUMBER 2081CT0)	
)	
and)	
)	
ELECTRONIC ITEMS RECOVERED FROM)	
BUILDING 197 OF THE WASHINGTON NAVY)	
YARD IN SOUTHWEST, D.C.)	
)	
and)	
)	
ELECTRONIC ITEMS RECOVERED IN A)	
BACKPACK FOUND IN BUILDING 197 OF)	
THE WASHINGTON NAVY YARD IN)	
SOUTHWEST, D.C.)	

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Special Agent Sarah Jones, being duly sworn, depose and state as follows:

I. INTRODUCTION AND SUMMARY OF PROBABLE CAUSE

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—that is, electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically-stored information described in Attachment B. For the reasons detailed below, I believe there is probable cause that the electronic devices were used by Aaron Alexis in relation to a mass shooting he perpetrated on September 16, 2013, at the Washington Navy Yard in Southwest, D.C. Moreover, I believe there is probable cause that the electronic devices may contain evidence related to the offenses of Murder, in violation of 18

U.S.C. § 1111, Attempted Murder, in violation of 18 U.S.C. § 1113, and Killing or Attempted Killing of officer or employee of United States, in violation of 18 U.S.C. § 1114.

2. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a warrant to search the electronic devices and to seize evidence, fruits, and instrumentalities of criminal activity that may be found within them, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth only those facts that I believe are sufficient to establish the necessary foundation for the search warrant.

3. I make this affidavit based upon (a) personal observations and knowledge; (b) conversations with other law enforcement agents who have participated in this investigation and related investigations; and (c) review of documents connected with the investigation. I believe the information received from others to be truthful and reliable to the best of my knowledge. Where I have reported statements made by others, or from documents that I have reviewed, those statements are reported in substance and in part, unless otherwise indicated.

II. AGENT BACKGROUND

4. I am a Federal Law Enforcement Agent, authorized to investigate violations of the laws of the United States, and I am a law enforcement officer with authority to execute arrest and search warrants issued under the authority of the United States.

5. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since February 2011. I am currently assigned to investigate computer crimes, with specific responsibility for computer intrusions, and have received training as such. Prior to my employment as a Special Agent with the FBI, I was a Management and Program Analyst for the FBI, managing programs and initiatives, writing policy, and analyzing existing data, trends, and mission needs. I am trained and authorized to investigate the offenses alleged herein. I received

training at the FBI's Special Agent Academy. I have received organizational sponsored computer training, and I am A+ certified (a certification for computer professionals). In addition, I have received basic and advanced computer training at the SANS institute. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C § 2510(7) and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C § 2516.

III. IDENTIFICATION OF THE ELECTRONIC DEVICES TO BE SEARCHED

6. The property to be searched is a laptop computer, further identified as a Lenovo Thinkpad T500 laptop computer, having serial number L3-B0317 09/02 and Product ID Number 2081CT0, and various electronic items recovered as evidence at the Washington Navy Yard in Southwest, D.C., further identified in Attachment A (collectively hereinafter the "Devices"). The owner of the Devices is believed to be Aaron Alexis, now deceased. The Lenovo Thinkpad T500 laptop computer is currently located at the Residence Inn at 333 E Street, Southwest, Washington, D.C., and the various electronic items recovered as evidence at the Washington Navy Yard in Southwest, D.C., are still located at the Navy Yard.

7. The applied-for warrant would authorize the forensic examination of the Devices described in Attachment A for the purpose of identifying electronically-stored data particularly described in Attachment B.

IV. FACTS ESTABLISHING PROBABLE CAUSE

8. On September 16, 2013, at approximately 8:12 am, there was a report of an "active shooter" at the Washington Navy Yard ("Navy Yard"), located in Southwest, Washington, D.C.

9. First Responders with the Naval Criminal Investigative Services ("NCIS") and

D.C. Metropolitan Police Department (the “First Responders”) responded to Building 197 of the Navy Yard to investigate the reported shooting. Upon arriving, the First Responders discovered multiple victims with visible gunshot wounds throughout Building 197, some of whom were dead and some of whom were injured.

10. NCIS personnel identified a suspected male shooter and exchanged gunfire with that individual inside Building 197. Later, members of the D.C. Metropolitan Police Department’s Emergency Response Team later arrived at the scene and also exchanged gunfire with the male shooter. In the ensuing gunfire, the male shooter was shot and killed.

11. Special Agents with the FBI’s Violent Crimes Task Force came to the scene and scanned the now-deceased male shooter’s fingers to obtain his fingerprints. Those fingerprints were then electronically compared against known fingerprints contained in a Criminal Justice Information Services Division database, which resulted in a positive fingerprint comparison to Aaron Alexis, having a date of birth of May 9, 1979, and a last known address in Fort Worth, TX 76108 (hereinafter “Alexis”).

12. Through various law enforcement databases, the FBI, in coordination with other law enforcement entities determined that Alexis was an employee of Experts IT, a subcontractor for a defense contracting company of the United States Department of Defense.

13. NCIS members subsequently determined that Experts IT had been providing information technology services at the Navy Yard, since approximately Monday, September 9, 2013. It was also determined that Alexis was one of Expert IT’s employees that was assigned to provide those services.

14. In connection with the services being provided by Experts IT to the Navy Yard, Alexis had been issued an access identification badge, which allowed Alexis access to the Navy

Yard and Building 197 at the Navy Yard. Further investigation also revealed that the access identification badge issued to Alexis had been used to access the Navy Yard on multiple occasions from September 9 through September 16, 2013. The last time Alexis's access identification badge was used to access Building 197 in the Navy Yard was at approximately 8:02 am on September 16, 2013.

15. In a search of Building 197, law enforcement agents found Alexis's access identification badge on the first floor of that location near a shotgun believed to have belonged to Alexis and used by him in the shooting.

16. Alexis's body was found on the third floor of Building 197. Near his body was 9mm semi-automatic pistol, also believed to be used by him in the shooting. The 9mm semi-automatic pistol was recovered from the crime scene, examined, and determined to be loaded.

17. Also recovered from the crime scene were multiple expended 9mm cartridge casings and shotgun shells, consistent with the firearms found on the scene and believed to be used by Alexis in the shooting.

18. To date, the investigation has revealed that the shooting at the Navy Yard resulted in thirteen (13) deceased victims, including Alexis, along with multiple other injured victims.

Devices Recovered During the Search of Building 197

19. During the course of a search of a bathroom located of the fourth floor of Building 197, where the shooting occurred, law enforcement recovered the below-listed electronic items inside a backpack and separate carrying case. In addition to the following electronic items, inside the backpack and carrying case were documents bearing the suspect's name, "Aaron Alexis." Also inside the backpack were empty boxes of ammunition, consistent with the caliber discharged on the scene. Video surveillance footage from Building 197 shows

Alexis entering this bathroom while appearing to carry the backpack and carrying case, and later emerging from the bathroom holding a shotgun. The electronic items found inside the backpack, included:

- 16GB micro SDHC, inside USB card reader;
- 4GB DataStick Pro, by Centon;
- 2GB ATP Tough Drive USB stick, serial number AF2GUFT3BK;
- Rosewill external hard drive, serial number 17182180040900232;
- CD-R, labeled aircraft PC training;
- CD-RW, labeled Microsoft Office 2010;
- DVD-R, unlabeled; and
- Mini DVD-R, labeled “unclassified,” “unclass,” and “migration” (with additional illegible writing).

The electronic items located inside the carrying case included:

- CD-R M.A.T-8.3.4;
- CD-R M.A.T-8.3.4;
- CD-R M.A.T- 8.3.4; and
- DVD-R SAV-DAT, labeled August 13, 2013.

Alexis’s Hotel Room at the Residence Inn

20. NCIS personnel also determined that employees with Experts IT, including Alexis, were residing temporarily at the Residence Inn at 333 E Street, SW, Washington, DC (hereinafter, the “Residence Inn”), while providing services to the Navy Yard pursuant to the above-referenced contract. NCIS personnel determined that Alexis was temporarily residing in room 716 of the Residence Inn.

21. FBI agents went to the Residence Inn and confirmed that Alexis had been staying in Room 716 since approximately Saturday, September 7, 2013.

22. On September 16, 2013, a Special Agent with the FBI applied for and obtained a search warrant from this Court for the search of Alexis's hotel room.

23. While executing the search warrant at Alexis's hotel room, FBI agents discovered and seized, among other things, the Lenovo Thinkpad T500 laptop computer. At the time it was discovered, the Lenovo Thinkpad T500 laptop computer was in and among other personal effects of Alexis, including items with Alexis's name on them (e.g., a Hertz rental car agreement). The FBI did not find any other property or information within Alexis's hotel room that would indicate that someone other than Alexis had been staying in the room or that any of the personal property, including the Lenovo Thinkpad T500 laptop computer, that was found there was owned by anyone other than Alexis.

24. The Navy Yard is within the special maritime and territorial jurisdiction of U.S.

V. EVIDENCE LIKELY TO BE OBTAINED IN SEARCH OF DEVICES

25. Based on my training and experience, and information provided to me by other law enforcement agents, I know that computer-related devices may be important to an investigation of violent crimes, particularly those involving premeditation and deliberation, in several distinct and important respects: First, electronic devices usually provide information that helps confirm the identity of the user(s) of the devices. Second, individuals intending to commit such violent crimes use computer-related devices to facilitate their illegal acts by, for example, conducting research on potential target(s), determining the manner in which to undertake their attacks on their identified target(s), and facilitate the means to effectively reach their target(s) (such as orchestrating travel arrangements to carrying out the attack). Third, computer-related

devices may be used to collect or store information about criminal activities (in the form of electronic data), such as names and contact numbers of possible co-conspirators. Fourth, when the criminal violations involve a degree of sophistication that may entail a conspiracy or multiple individuals, a search of the electronic device of one of the participants often allows law enforcement officials to identify other participants or co-conspirators, based on a suspect's use of the device to communicate with those additional participants.

26. Here, a review of the electronically-stored communications and other information in the Devices will enable the FBI to find, among other things, any evidence of research and planning by Alexis, as well as help identify any co-conspirators or accomplices to the offenses.

VI. CONCLUSION

27. Based on the facts and for the reasons set forth above, I respectfully submit that there is probable cause to search the Devices.

28. The materials sought to be seized constitute evidence, fruits or instrumentalities related to violation of federal criminal law, including but not limited Murder, in violation of 18 U.S.C. § 1111, Attempted Murder, in violation of 18 U.S.C. § 1113, and Killing or Attempted Killing of officer or employee of United States, in violation of 18 U.S.C. § 1114, as set forth more fully in Attachment B.

Sarah Jones
Special Agent
Federal Bureau Investigation

Subscribed and sworn to before me
telephonically pursuant to Rule 4.1 of
the Federal Rule of Criminal Procedure
on September ____, 2013

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DEVICES TO BE SEARCHED

Electronic items located inside a carrying case found in Building 197:

- CD-R M.A.T-8.3.4;
- CD-R M.A.T-8.3.4;
- CD-R M.A.T- 8.3.4; and
- DVD-R SAV-DAT, labeled August 13, 2013.

ATTACHMENT B

ITEMS TO BE SEIZED

All evidence, fruits, and instrumentalities stored in the Devices, related to the offenses of Murder, in violation of 18 U.S.C. § 1111, Attempted Murder, in violation of 18 U.S.C. § 1113, and Killing or Attempted Killing of officer or employee of United States, in violation of 18 U.S.C. § 1114, including but not limited to:

1. Records and information, and items related to violations of the aforementioned statutes;
2. Records, information, and items related to the identity of Aaron Alexis;
3. Records, information, and items related to the Washington Navy Yard or individuals working or present there;
4. Records, information, and items related to any targeting of, or planning to attack the Washington Navy Yard or individuals working or present there, or any records or information related to any past attacks;
5. Records, information, and items related to the state of mind of Alexis, or any other individuals seeking to undertake any such attack and/or the motivations for the attack;
6. Records, information, and items related to any organization, entity, or individual in any way affiliated with Alexis;
7. Records, information, and items related to any associates of Alexis or other individuals he communicated with about his planned violent attacks, including the one perpetrated at the Washington Navy Yard on September 16, 2013;
8. Records, information, and items related to Alexis or his associates' schedule of travel or travel documents;
9. Records, information, and items related to any firearms or ammunition;
10. Any firearms or ammunition;
11. Records, information, and items related to any bank records, checks, credit card bills, account information, and other financial records;
12. All digital evidence, as that term is used herein, means the following:

- (a) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the Device or data to be searched;
- (b) Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the Devices or data;
- (c) Any passwords, password files, test keys, encryption codes, or other information necessary to access the Devices of data; and
- (d) All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on the Devices, that shows the actual user(s) of the Devices during the time the Devices was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the Devices; MAC IDs and/or Internet Protocol addresses used by the Devices; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the Devices such as viruses, Trojan horses, and other forms of malicious software.

DIGITAL EVIDENCE SEARCH PROCEDURE

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

- (A) Law enforcement personnel will examine the Devices to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in this Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.
- (B) Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.
- (C) If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on the Devices do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may

continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.